

УДК 512.62

МАТЕМАТИКА

М. К. Кюрегян

К теории приводимости полиномов над конечными полями

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 18/IX 1987)

Пусть F_q — поле Галуа порядка $q = p^s$, p — простое число, s — натуральное число.

Введем в рассмотрение оператор Р. Р. Варшамова (1)

$$I^{\theta} f(x) = \frac{1}{\theta(x)} \sum_{u=0}^n \sum_{v=0}^m a_u \theta_v x^{u+q^v},$$

где $f(x) = \sum_{u=0}^n a_u x^u$ и $\theta(x) = \sum_{v=0}^m \theta_v x^v$ ($\theta(x) \neq 0$), a_u и $\theta_v \in F_q$.

В настоящей работе разработан новый метод построения неприводимых полиномов в явном виде над полями Галуа с помощью известной теоремы Р. Р. Варшамова, которая гласит: если $\theta(x) = \varepsilon(x)L^{\lambda}(x) + \delta$, где $\varepsilon(x)$ — произвольный полином над полем F_q , $i(x)$ и $f(x)$ — полиномы с ненулевыми свободными членами над полем F_q , $f(1) \neq 0$, δ — произвольный элемент поля F_q , $K(i_u, f_u) = L^{\lambda} L^{\lambda(i_u)} i_u(x) f_u(x)$, где $i_u(x) | i(x)$, $f_u(x) | f(x)$, $i_u(x) f_u(x) \neq (x) f(x)$, $\varepsilon(\delta) = \delta^{q-1} x - 1$ и N — период полинома $S(x) = \varepsilon(\delta) i(x) f(x)$, то степень $g(x)$ любого неприводимого делителя $L^{\lambda} f(x)$, удовлетворяющего условию $g(x) \cdot K(i_u, f_u)$, кратна $N^{(1-2)}$.

Будем говорить, что степень элемента β над полем F_q равна k или же β является собственным элементом поля F_{q^k} , если $\beta \in F_{q^k}$ и $\beta \notin F_{q^d}$, где d — любой собственный делитель k . В этом случае пишем: $\deg_q(\beta) = k$.

В работе рассматриваются только нормированные полиномы, т. е. полиномы, старший коэффициент которых равен единице.

Теорема 1. Пусть p — простое нечетное число, α — произвольный примитивный элемент поля F_p , δ — произвольный элемент поля F_p . Тогда полином $H(x) = \sum_{u=0}^{p-1} x^{p(p-u-1)} (\alpha x + \delta)^u - \alpha$ степени $p(p-1)$ неприводим над полем F_p .

Доказательство. Легко видеть, что $\sum_{u=0}^{p-1} x^{p(p-u-1)} (\alpha x + \delta)^u - \alpha = (x^p - \alpha x + \delta)^{p-1} - \alpha = L^{\lambda} L^{\lambda(i)} i(x) f(x)$, где $i_u(x) | x - \alpha$, $f_u(x) | x - \alpha$, $i_u(x) f_u(x) \neq (x - \alpha)^2$ и $\varepsilon(\delta) = \delta^{p-1} x - 1$. В самом деле, из того, что

$$L^x(x-1)(x-a)^2 = L^x(x-1)L^{xL^x(x-1)}(x-a)L^{xL^x(x-1)(x-a)}(x-a) \quad (1)$$

и учитывая, что $L^x(x-1)(x-a)^2$ сепарабельный полином ⁽²⁾, имеем

$$(L^{xL^x(x-1)}(x-a), L^{xL^x(x-1)(x-a)}(x-a)) = 1.$$

Однако согласно ⁽²⁾

$$L^{xL^x(x-1)(x-a)}(x-a) = \prod_{\delta \in F_p} L^{xL^x(x-a)+\delta}(x-a) \quad \text{и}$$

$$L^{xL^x(x-1)}(x-a) = \prod_{\delta \in F_p} L^{x+\delta}(x-a),$$

а это означает, что согласно (1)

$$(L^{xL^x(x-1)}(x-a), L^{xL^x(x-a)+\delta}(x-a)) = 1$$

для любого $\delta \in F_p$. Кроме того, $L^{xL^{x+\delta}(x-a)+\delta}(x-a) = 1$, следовательно, $(L^{xL^x(x-a)+\delta}(x-a), H(x)) = 1$.

Заметим, что показатель $p(p-1)$ полинома $e(\delta)(x-a)^2$ совпадает со степенью $H(x)$, поэтому согласно теореме Р. Р. Варшамова ⁽²⁾ полином $H(x)$ неприводим над полем F_p .

Теорема 2. Пусть p — простое нечетное число, x — произвольный примитивный элемент поля F_p , δ — произвольный элемент поля F_p , $f(x)$ — неприводимый над полем F_p полином степени n такой, что $(n, p(p-1)) = 1$, $x^{p^2} - 2\alpha x^p + \alpha^2 x = R(x) \pmod{f(x)}$, $x^p - \alpha x \equiv V(x) \pmod{f(x)}$, $\psi(x) = \sum_{u=0}^n \psi_u x^u$ и $\varphi(x) = \sum_{u=0}^n \varphi_u x^u$, где ψ_u и φ_u — нетривиальные решения сравнений

$$\sum_{u=0}^n \psi_u (R(x))^u \equiv 0 \pmod{f(x)} \quad \text{и} \quad \sum_{u=0}^n \varphi_u (V(x))^u \equiv 0 \pmod{f(x)} \quad (2)$$

соответственно. Тогда полиномы $\psi(x)$, $\varphi(x)$ степени n и полином

$$F(x) = \frac{\psi(x^{p^2} - 2\alpha x^p + \alpha^2 x + \delta(1-\alpha))}{\varphi(x^p - \alpha x + \delta)} \quad (3)$$

степени $pr(p-1)$ неприводимы над полем F_p .

Доказательство. Сначала докажем теорему для случая $n=1$. Пусть $f(x) = x + a$. Учитывая, что $x^{p^2} - 2\alpha x^p + \alpha^2 x = (x+a)((x+a)^{p^2-1} - 2\alpha(x+a)^{p-1} + \alpha^2(x+a)) - a(1-\alpha)^2$ и $x^p - \alpha x = (x+a)((x+a)^{p-1} - \alpha(x+a)) - a(1-\alpha)$, имеем: $(R(x))^0 = 1$, $R(x) = -a(1-\alpha)^2$, и $(V(x))^0 = 1$, $V(x) = -a(1-\alpha)$. Согласно сравнениям (2) коэффициенты полиномов $\psi(x)$ и $\varphi(x)$ будут иметь вид: $\psi_0 = a(1-\alpha)^2$, $\psi_1 = 1$ и $\varphi_0 = -a(1-\alpha)$, $\varphi_1 = 1$, соответственно, следовательно, $\psi(x) = x + a(1-\alpha)^2$ и $\varphi(x) = x + a(1-\alpha)$. Таким образом,

$$F(x) = \frac{x^{p^2} - 2\alpha x^p + \alpha^2 x - \delta(1-\alpha) + a(1-\alpha)^2}{x^p - \alpha x + \delta + a(1-\alpha)} = ((x+a)^p - \alpha(x+a) + \delta)^{p-1} - a,$$

однако последний полином согласно теореме 1 неприводим над полем F_p . Рассмотрим теперь случай, когда $n > 1$.

По теореме 1 полином $H(x) = (x^p - \alpha x + \delta)^{p-1} - a = \frac{x^{p^2} - 2\alpha x^p + \alpha^2 x + \delta(1-\alpha)}{x^p - \alpha x + \delta}$ неприводим над полем F_p . Так как $(n,$

$p(p-1)=1$, то полином $H(x)$ неприводим также и над полем F_{p^n} . Поэтому, если γ —корень уравнения $f(x)=0$, то среди коэффициентов полинома $H(x-\gamma)=h(x)=\sum_{v=0}^{p(p-1)} h_v x^v$ согласно (3), поскольку $n>1$, найдется хотя бы один коэффициент h_v такой, что $\deg_p(h_v)=n$. Далее, вследствие того, что $h^{(u)}(x)=H(x-\gamma^{p^u})=\sum_{v=0}^{p(p-1)} h_v^{p^u} x^v$, согласно (4)

полином $H_1(x)=\prod_{u=0}^{n-1} h^{(u)}(x)$ неприводим над полем F_p . Стало быть

$$H_1(x) = \frac{\prod_{u=0}^{n-1} (x^{p^u} - 2\alpha x^{p^u} + \alpha^2 x + \delta(1-\alpha) - (\gamma^{p^u} - 2\alpha\gamma^{p^u} + \alpha^2\gamma)^{p^u})}{\prod_{u=0}^{n-1} (x^p - \alpha x + \delta - (\gamma^p - \alpha\gamma)^{p^u})}. \quad (4)$$

Покажем теперь, что элементы $\gamma^{p^2} - 2\alpha\gamma^{p^2} + \alpha^2\gamma = \xi$ и $\gamma^p - \alpha\gamma = \beta$ являются собственным элементом поля F_{p^n} . Допустим противное, а именно предположим, что максимальные степени элементов ξ и β над полем F_p равны k и m соответственно, т. е. $\deg_p(\xi) = k$ и $\deg_p(\beta) = m$, где k и m —собственные делители n . Тогда $\prod_{u=0}^{n-1} (x - \xi^{p^u}) = (\psi(x))^N$ и $\prod_{u=0}^{n-1} (x - \beta^{p^u}) = (\varphi(x))^M$, где $n = kN$ ($N>1$) и $n = mM$ ($M>1$). Следовательно, согласно (4) будем иметь

$$H_1(x) = \frac{(\psi(x^{p^2} - 2\alpha x^{p^2} + \alpha^2 x + \delta(1-\alpha)))^N}{(\varphi(x^p - \alpha x + \delta))^M}. \quad (5)$$

Отсюда, поскольку полином $H_1(x)$ неприводим над полем F_p , имеем $H_1(x) | \psi(x^{p^2} - 2\alpha x^{p^2} + \alpha^2 x + \delta(1-\alpha))$, но тогда $np(p-1) \leq kp^2$, что невозможно. Значит, $N=1$ и ξ является собственным элементом поля F_{p^n} , что в свою очередь устанавливает неприводимость полинома $\psi(x) = \prod_{u=0}^{n-1} (x - \xi^{p^u})$ над полем F_p . Покажем, что $M=1$. Действительно, по теореме Варшамова (2) нетрудно убедиться в том, что полином

$$Q(x) = \left(x - \frac{\delta}{\alpha-1} \right)^{p-1} - \alpha = \frac{x^p - \alpha x + \delta}{x - \frac{\delta}{\alpha-1}}$$

теперь, так как $(n, p-1)=1$, полином $Q(x)$ неприводим также и над полем F_{p^n} . Тогда среди коэффициентов полинома $Q(x-\gamma)=g(x)=\sum_{u=0}^{p-1} g_u x^u$ согласно (3), поскольку $n>1$, найдется хотя бы один коэффициент g_u такой, что $\deg_p(g_u)=n$. Если учесть также следующую легко доказываемую формулу $Q(x-\gamma^{p^u})=g^{(u)}(x)=\sum_{v=0}^{p-1} g_v^{p^u} x^v$, то

согласно (4) полином $Q_1(x)=\prod_{u=0}^{n-1} g^{(u)}(x)$ будет неприводим над полем

F_p . Следовательно, будем иметь $Q_1(x)f\left(x - \frac{\delta}{a-1}\right) = (\psi(x^p - ax + \delta))^{M_1}$, но поскольку полиномы $Q_1(x)$ и $f\left(x - \frac{\delta}{a-1}\right)$ неприводимы над полем F_p , то имеем $M_1 = 2$ и $n = n(p-1)$, что невозможно. Следовательно, $M_1 = 1$, а β является собственным элементом поля F_{p^n} , что в свою очередь устанавливает неприводимость полинома $\varphi(x) = \prod_{u=0}^{n-1} (x - \beta^{p^u})$ над полем F_p . Таким образом, в силу (5) полином (3) будет неприводим над полем F_p . Наконец, нетрудно убедиться в том, что $\psi(R(x)) \equiv 0 \pmod{f(x)}$ и $\varphi(V(x)) \equiv 0 \pmod{f(x)}$ или $\sum_{u=0}^n \psi_u(R(x))^u \equiv 0 \pmod{f(x)}$ и $\sum_{u=0}^n \varphi_u(V(x))^u \equiv 0 \pmod{f(x)}$. Теорема доказана.

Лемма. Пусть $f(x) = \sum_{u=0}^n a_u x^u$ — произвольный неприводимый над полем F_q полином степени n , принадлежащий показателю e , и среди коэффициентов a_1, a_{n-1} найдется хотя бы один, не равный нулю, $t|q-1$, $x^t \equiv R(x) \pmod{f(x)}$ и $\psi(x) = \sum_{u=0}^n \psi_u x^u$, где ψ_u — не тривиальное решение сравнения

$$\sum_{u=0}^n \psi_u (R(x))^u \equiv 0 \pmod{f(x)}. \quad (6)$$

Тогда полином $\psi(x)$ степени n не будет разлагаться над полем F_q и принадлежит показателю $\frac{e}{(t, e)}$.

Доказательство. Пусть γ — корень уравнения $f(x) = 0$. Учитывая (6), нетрудно убедиться в том, что γ^t будет корнем $\psi(x)$. Теперь достаточно показать, что γ^t является собственным элементом поля F_{q^n} . Допустим противное, а именно предположим, что максимальная степень элемента γ^t над полем F_q равна r , т. е. $\deg_q(\gamma^t) = r$, где r — собственный делитель n .

Рассмотрим отдельно два возможных случая.

1. Пусть $a_1 \neq 0$. Поскольку согласно теореме Виетта имеем $\sum_{u=0}^{n-1} (\gamma^{-1})^{q^u} = -\frac{a_1}{a_0}$ или $\gamma^{-1} \sum_{u=0}^{n-1} (\gamma^{-1})^{q^u-1} = -\frac{a_1}{a_0}$, то, так как $t|q^n-1$, будем иметь $(\gamma^{-1})^{q^n-1} \in F_{q^r}$, а это значит, $\sum_{u=0}^{n-1} (\gamma^{-1})^{q^u-1} \in F_{q^r}$. Ввиду того, что $\gamma = -\frac{a_0}{a_1} \sum_{u=0}^{n-1} (\gamma^{-1})^{q^u-1} \in F_{q^r}$, будем иметь $\deg_q(\gamma) < n$, что невозможно.

2. Пусть $a_{n-1} \neq 0$. Тогда, имея в виду, что $\sum_{u=0}^{n-1} \gamma^{q^u} = -a_{n-1}$ или же $\gamma \sum_{u=0}^{n-1} \gamma^{q^u-1} = -a_{n-1}$ и $t|q^n-1$, получим $\gamma = -\left(\sum_{u=0}^{n-1} \gamma^{q^u-1}\right)^{-1} a_{n-1} \in F_{q^r}$ и, следовательно, $\deg_q(\gamma) < n$, что также невозможно. Лемма доказана.

Теорема 3. Пусть $\delta \neq 0$ — произвольный элемент поля F_q , $f(x) = \sum_{u=0}^n a_u x^u$ неприводимый над полем F_q полином степени n , коэффициенты которого удовлетворяют условию $\sum_{u=0}^{s-1} \left(\frac{a_1 \delta}{a_0} \right)^{q^u} \neq 0$, $x^{p-1} \equiv R(x) \pmod{f(x)}$, $\psi(x) = \sum_{u=0}^n \psi_u x^u$, где ψ_u — нетривиальное решение уравнения $\sum_{u=0}^n (R(x))^u \equiv 0 \pmod{f(x)}$ и $\psi_1 = 1$. Тогда полином $F(x) = x^n \psi \left(\frac{x^p - \delta^p}{x} \right)$ неприводим над полем F_q .

Доказательство. Согласно лемме полином $\psi(x)$ неприводим над полем F_q и $\psi(\gamma^{p-1}) = 0$ ($f(\gamma) = 0$). Теперь, используя (5), получим, что $x^n \psi \left(\frac{x^p - \delta^p}{x} \right)$ неприводим над полем F_q , если γ^{p-1} и δ удовлетворяют условию $\sum_{u=0}^{ns-1} \delta^{p^{u+1}} \gamma^{p^{us} - p^{u+1}} \neq 0$. Упростим это условие. Легко видеть, что $\sum_{u=0}^{ns-1} \delta^{p^{u+1}} \gamma^{p^{us} - p^{u+1}} = \gamma \left(\sum_{u=0}^{s-1} \left(\sum_{v=0}^{n-1} (\delta \gamma^{-1})^{p^{sv}} \right)^{p^u} \right)^p$ и $f(\delta x) = \sum_{u=0}^n a_u (\delta x)^u = \sum_{u=0}^n h_u x^u$. Отсюда $h_1 = a_1 \delta$ и согласно теореме Виетта $\sum_{u=0}^{s-1} \left(\sum_{v=0}^{n-1} (\delta \gamma^{-1})^{p^{sv}} \right)^{p^u} = \sum_{u=0}^{s-1} \left(-\frac{a_1 \delta}{a_0} \right)^{p^u}$. Таким образом, если $\sum_{u=0}^{s-1} \left(\frac{a_1 \delta}{a_0} \right)^{p^u} \neq 0$, то полином $x^n \psi \left(\frac{x^p - \delta^p}{x} \right)$ неприводим над полем F_q . Теорема доказана.

Опираясь на теорему 3 и используя работу (6), можно будет доказать следующий факт.

Теорема 4. Пусть $\delta \neq 0$ — произвольный элемент поля F_{2^s} , $f(x) = \sum_{u=0}^n a_u x^u$ — неприводимый над полем F_{2^s} полином степени n , коэффициенты которого удовлетворяют условиям $\sum_{u=0}^{s-1} \left(\frac{a_1 \delta}{a_0} \right)^{2^u} = 1$ и $\sum_{u=0}^{s-1} \left(\frac{a_{n-1}}{\delta} \right)^{2^u} = 1$, $b_m(x)$ и $c_m(x)$ ($m \geq 1$) — последовательности функций, заданных рекуррентными уравнениями $b_m(x) = (b_{m-1}(x))^2 + (\delta c_{m-1}(x))^2$, $c_m(x) = b_{m-1}(x) c_{m-1}(x)$ при начальных условиях $b_1(x) = x^2 + \delta^2$, $c_1(x) = x$. Тогда для произвольного натурального m полином $F(x) = \sum_{u=0}^n a_u b_m^u(x) c_m^{n-u}(x)$ степени $2^m n$ будет неприводим над полем F_{2^s} .

Автор считает своим приятным долгом выразить благодарность чл.-корр. АН Армянской ССР Р. Р. Варшамову за полезные советы в процессе работы над статьей.

Վերջավոր դաշտերի վրա բազմանդամների
վերածելիության տեսության մասին

Աշխատանքում հետազոտվում են մի քանի ձևափոխություններ, որոնց համար որպես որոշման տիրույթ հանդիսանում է Գալուայի F_n դաշտից վերցված գործակիցներով բազմանդամների օղակը: Ապացուցվում են մի շարք թեորեմներ, որոնք հնարավորություն են տալիս անվերծանելի բազմանդամներ կառուցել բացահայտ տեսքով Գալուայի F_n կամայական դաշտի վրա: Բացի այդ, վերջում տրվում է F_{2^k} վերջավոր դաշտի վրա $2^m n$ -րդ աստիճանի (որտեղ m -ը՝ կամայական բնական թիվ է) անվերծանելի բազմանդամների կառուցման մի ռեկուրենտ եղանակ:

ЛИТЕРАТУРА—ԳՐԱԿԱՆՈՒԹՅՈՒՆ

¹ P. P. Варшамов, ДАН СССР, т. 156, № 6 (1964). ² P. P. Варшамов, ДАН Арм. ССР, т. 79, № 1 (1984). ³ М. К. Кюрегян, ДАН АрмССР, т. 83, № 2 (1986). ⁴ М. К. Кюрегян, ДАН АрмССР, т. 81, № 2 (1985). ⁵ М. К. Кюрегян, ДАН АрмССР, т. 83, № 4 (1986). ⁶ М. К. Кюрегян, ДАН АрмССР, т. 84, № 2 (1987).